AMENDMENTS TO THE CLAIMS

Claim 1 (Currently Amended) An encryption communication system for secret message communication, the encryption communication system comprising an encryption transmission apparatus and an encryption reception apparatus, ~~wherein~~

wherein the encryption transmission apparatus includes:

a storage unit that stores ~~therein~~ one message;

an encryption unit operable to perform an encryption computation on the one message a plural number of times, ~~thereby generating ciphertexts~~ to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption unit being equal ~~in number~~ to the number of times ~~of~~ the encryption unit performs the encryption computation on the one message;

a computation unit operable to perform a one-way operation on the one message, ~~thereby generating~~ to generate a comparison computation value; and

a transmission unit operable to transmit, to the encryption reception apparatus, the plurality of the encrypted messages ~~the ciphertexts~~ and the comparison computation value, and

wherein the encryption reception apparatus includes:

a reception unit operable to receive, from the encryption transmission apparatus, the plurality of the encrypted messages ~~the ciphertexts~~ and the comparison computation value;

a decryption unit operable to perform a decryption computation, ~~which corresponds~~ corresponding to the encryption computation, the decryption computation being performed on each of the encrypted messages to generate a plurality of ~~ciphertexts, thereby generating~~ decrypted messages, and a number of decrypted messages generated by the

decryption unit being equal ~~in number~~ to the number of ~~the~~ encrypted messages generated from the one message by the encryption unit ~~ciphertexts~~;

a computation unit operable to perform the one-way operation on each of the decrypted messages to generate a plurality of~~, thereby generating~~ decryption computation values, a number of decryption values generated by the computation unit being equal ~~in number~~ to the number of the decrypted messages generated by the decryption unit; and

a judging unit operable to compare each of the decryption computation values with the received comparison computation value,

wherein (i) when ~~and i) if~~ at least one of the decryption computation values matches the received comparison computation value, the judging unit outputs ~~output a corresponding~~ decrypted message ~~text, and ii) if~~, and (ii) when none of the decryption computation values matches the received comparison computation value, the judging unit ~~output~~ determines that there is a decryption error.

Claim 2 (Currently Amended) The encryption communication system of Claim 1, ~~wherein~~

wherein the encryption computation used by the encryption unit conforms to NTRU cryptosystem, and

wherein the decryption computation used by the decryption unit conforms to the NTRU cryptosystem.

Claim 3 (Currently Amended) An encryption transmission apparatus for secret message communication with an encryption reception apparatus, the encryption transmission apparatus

comprising:

a storage unit that stores ~~therein~~ one message;

an encryption unit operable to perform an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, ~~thereby generating ciphertexts~~, a number of encrypted messages generated from the one message by the encryption unit being equal ~~in number~~ to the number of times ~~of~~ the encryption unit performs the encryption computation on the one message;

a computation unit operable to perform a one-way operation on the one message, ~~thereby generating~~ to generate a comparison computation value; and

a transmission unit operable to transmit, to the encryption reception apparatus, the plurality of the encrypted messages ~~ciphertexts~~ and the comparison computation value.

Claim 4 (Currently Amended) The encryption transmission apparatus of Claim 3, wherein the encryption unit comprises:

an encryption computation subunit operable to perform an invertible data conversion on the one message to generate ~~thereby generating~~ a converted message, and perform an encryption algorithm on the converted message to generate one encrypted message ~~thereby generating a ciphertext~~; and

a repetition control subunit operable to control the encryption computation subunit to repeat the generation of the converted message and the generation of the one encrypted message ~~ciphertext~~, the generation of the converted message and the generation of the one encrypted message being repeated the plural number of times the encryption unit performs the encryption

computation on the one message to generate the plurality of encrypted messages.

Claim 5 (Currently Amended) The encryption transmission apparatus of Claim 4, wherein the encryption computation subunit generates a random number of a fixed length, and generates the converted message by adding the random number to the one message.

Claim 6 (Currently Amended) The encryption transmission apparatus of Claim 5, wherein the encryption algorithm used by the encryption computation subunit on the converted message conforms to NTRU cryptosystem.

Claim 7 (Currently Amended) An encryption reception apparatus for secret message communication with an encryption transmission apparatus, ~~where~~ the encryption transmission apparatus storing ~~stores therein~~ one message, ~~performs~~ performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message ~~thereby generating ciphertexts~~, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal ~~in number~~ to the number of times ~~of~~ the encryption transmission apparatus performs the encryption computation on the one mesasage, ~~performs~~ performing a one-way operation on the one message to generate ~~thereby generating~~ a comparison computation value, and ~~transmits~~ transmitting, to the encryption reception apparatus, the plurality of encrypted messages ~~the ciphertexts~~ and the comparison computation value, the encryption reception apparatus comprising:

a reception unit operable to receive, from the encryption transmission apparatus, the

plurality of the encrypted messages ~~the ciphertexts~~ and the comparison computation value;

a decryption unit operable to perform a decryption computation~~, which corresponds~~ corresponding to the encryption computation, the decryption computation being performed on each of the encrypted messages to generate a plurality of ~~the ciphertexts, thereby generating~~ decrypted messages, and a number of decrypted messages generated by the decryption unit being equal ~~in number~~ to the number of ~~the~~ encrypted messages generated from the one message by the encryption transmission apparatus ~~ciphertexts~~;

a computation unit operable to perform the one-way operation on each of the decrypted messages to generate a plurality of~~, thereby generating~~ decryption computation values, a number of decryption computation values generated by the computation unit being equal ~~in number~~ to the number of the decrypted messages generated by the decryption unit; and

a judging unit operable to compare each of the decryption computation values with the received comparison computation value,

wherein (i) when ~~and i) if~~ at least one of the decryption computation values matches the received comparison computation value, the judging unit outputs ~~output a corresponding~~ decrypted message ~~text, and ii) if~~, and (ii) when none of the decryption computation values matches the received comparison computation value, the judging unit ~~output~~ determines that there is a decryption error.

Claim 8 (Currently Amended) The encryption reception apparatus of Claim 7, ~~wherein~~ wherein the encryption transmission apparatus performs an invertible data conversion on the one message to generate ~~thereby generating~~ a converted message, performs an encryption

algorithm on the converted message to generate one encrypted message ~~thereby generating a ciphertext~~, and repeats the generation of the converted message and the generation of the one encrypted message ~~ciphertext~~, the generation of the converted one message and the generation of the one encrypted message being repeated the plural number of times the encryption unit performs the encryption computation on the one message to generate the plurality of encrypted messages, and ~~wherein~~

wherein the decryption unit comprises:

a decryption computation subunit operable to perform a decryption algorithm, ~~which corresponds~~ corresponding to the encryption algorithm, on one of the plurality of the encrypted messages to generate one decrypted text ~~a ciphertext thereby generating a decrypted text~~, and perform an inverse conversion of the invertible data conversion on the one decrypted text to generate one decrypted message ~~thereby generating a decrypted message~~; and

a repetition control subunit operable to control the decryption computation subunit to repeat the generation of the one decrypted content and the generation of the one decrypted message, the generation of the one decrypted content and the generation of the one decrypted message being repeated the plural number of times the decryption unit performs the decryption computation to generate the plurality of the decrypted messages being equal in number to the number of encrypted messages generated from the one message by the encryption unit.

Claim 9 (Currently Amended) The encryption reception apparatus of Claim 8, ~~wherein~~

wherein the encryption transmission apparatus generates a random number of a fixed

length, and generates the converted message by adding the random number to the one message, and ~~wherein~~

wherein the decryption computation subunit generates the one decrypted message by removing the random number of the fixed length from the one decrypted text ~~content~~.

Claim 10 (Currently Amended) The encryption reception apparatus of Claim 9, ~~wherein~~

wherein the encryption algorithm used by the encryption transmission apparatus conforms to NTRU cryptosystem, and ~~wherein~~

wherein the decryption algorithm used by the decryption computation subunit conforms to the NTRU cryptosystem.

Claim 11 (Currently Amended) An encryption transmission method used in an encryption transmission apparatus, the encryption transmission apparatus storing ~~that stores therein~~ one message and transmitting ~~transmits~~ the one message in secrecy to an encryption reception apparatus, the encryption transmission method comprising:

~~an encryption step of~~ performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message~~, thereby generating ciphertexts~~, a number of encrypted messages generated from the one message by the performing of the encryption computation being equal ~~in number~~ to the number of times ~~of~~ the performing of the encryption computation performs the ~~encrypted~~ encryption computation on the one message;

~~a computation step of~~ performing a one-way operation on the one message to generate~~,~~

~~thereby generating~~ a comparison computation value; and

~~a transmission step of~~ transmitting, to the encryption reception apparatus, the plurality of the encrypted messages ~~the ciphertexts~~ and the comparison computation value.

Claim 12 (Currently Amended) ~~An~~A computer-readable recording medium having an encryption transmission program recorded thereon, the encryption transmission program being used in an encryption transmission apparatus, the encryption transmission apparatus storing ~~that stores therein~~ one message and transmitting ~~transmits~~ the message in secrecy to an encryption reception apparatus, the encryption transmission program causing the encryption transmission apparatus to execute a method comprising:

~~an encryption step of~~ performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, ~~thereby generating ciphertexts~~, a number of encrypted messages generated from the one message by the performing of the encryption computation being equal ~~in number~~ to the number of times ~~of~~ the performing of the encryption performs the ~~encrypted~~ encryption computation on the one message;

~~a computation step of~~ performing a one-way operation on the one message to generate, ~~thereby generating~~ a comparison computation value; and

~~a transmission step of~~ transmitting, to the encryption reception apparatus, the plurality of the encrypted messages ~~the ciphertexts~~ and the comparison computation value.

Claim 13 (Cancelled)

Claim 14 (Currently Amended) An encryption reception method used in an encryption reception apparatus ~~that receives~~, the encryption reception apparatus receiving a message from an encryption transmission apparatus in secrecy, the encryption transmission apparatus storing ~~where the encryption transmission apparatus stores the~~ one message ~~therein~~, performing ~~performs~~ an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message ~~thereby generating ciphertexts~~, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal ~~in number~~ to the number of times ~~of~~ the encryption transmission apparatus performs the encryption computation on the one message, ~~performs~~ performing a one-way operation on the one message to generate ~~thereby generating~~ a comparison computation value, and ~~transmits~~ transmitting, to the encryption reception apparatus, the plurality of encrypted messages ~~the ciphertexts~~ and the comparison computation value, the encryption reception method comprising:

~~a reception step of~~ receiving, from the encryption transmission apparatus, the plurality of the encrypted messages ~~the ciphertexts~~ and the comparison computation value;

~~a decryption step of~~ performing a decryption computation corresponding~~, which corresponds~~ to the encryption computation, the decryption computation being performed on each of the encrypted messages to generate a plurality of ~~ciphertexts, thereby generating~~ decrypted messages, and a number of decrypted messages generated by the performing of the decryption computation being equal ~~in number~~ to the number of ~~the~~ encrypted messages generated from the one message by the encryption transmission apparatus ~~ciphertexts~~;

~~a computation step of~~ performing the one-way operation on each of the decrypted

messages to generate a plurality of~~, thereby generating~~ decryption computation values, a number of decryption computation values generated by the performing of the one-way operation being equal ~~in number~~ to the number of the decrypted messages generated by the performing of the decryption computation; ~~and~~

~~a judging step of comparing the decryption computation values with the received comparison computation value, and i) if at least one of the decryption computation values matches the received comparison computation value, outputting a corresponding decrypted message as a correct decrypted text, and ii) if none of the decryption computation values matches the received comparison computation value, outputting a decryption error~~

comparing each of the decryption computation values with the received comparison computation value;

outputting a decrypted message that corresponds to a decryption computation value that matches the received comparison value, based on the comparing, as a correct decrypted message when at least one of the plurality of the decryption computation values matches the received comparison computation value; and

determining that there is a decryption error when, as a result of the comparing, none of the decryption computation values matches the received comparison computation value.

Claim 15 (Currently Amended) ~~An~~A computer-readable recording medium having an encryption reception program recorded thereon, the encryption reception program being used in an encryption reception apparatus ~~that receives~~, the encryption reception apparatus receiving a message from an encryption transmission apparatus in secrecy, the encryption transmission

apparatus storing ~~where the encryption transmission apparatus stores the~~ one message ~~therein~~, performing ~~performs~~ an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message ~~thereby generating ciphertexts~~, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal ~~in number~~ to the number of times ~~of~~ the encryption transmission apparatus performs the encryption computation on the one message, ~~performs~~ performing a one-way operation on the one message to generate ~~thereby generating~~ a comparison computation value, and ~~transmits~~ transmitting, to the encryption reception apparatus, the plurality of encrypted messages ~~the ciphertexts~~ and the comparison computation value, the encryption reception program comprising:

~~a reception step of~~ receiving, from the encryption transmission apparatus, the plurality of the encrypted messages ~~the ciphertexts~~ and the comparison computation value;

~~a decryption step of~~ performing a decryption computation corresponding~~, which corresponds~~ to the encryption computation, the decryption computation being performed on each of the encrypted messages to generate a plurality of ~~ciphertexts, thereby generating~~ decrypted messages, and a number of decrypted messages generated by the performing of the decryption computation being equal ~~in number~~ to the number of ~~the~~ encrypted messages generated from the one message by the encryption transmission apparatus ~~ciphertexts~~;

~~a computation step of~~ performing the one-way operation on each of the decrypted messages to generate a plurality of~~, thereby generating~~ decryption computation values, a number of decrypted computation values generated by the performing of the one-way operation being equal ~~in number~~ to the number of the decrypted messages generated by the performing of the

decryption computation; ~~and~~

~~a judging step of comparing the decryption computation values with the received comparison computation value, and i) if at least one of the decryption computation values matches the received comparison computation value, outputting a corresponding decrypted message as a correct decrypted text, and ii) if none of the decryption computation values matches the received comparison computation value, outputting a decryption error~~

comparing each of the decryption computation values with the received comparison computation value;

outputting a decrypted message that corresponds to a decryption computation value that matches the received comparison value, based on the comparing, as a correct decrypted message when at least one of the plurality of the decryption computation values matches the received comparison computation value; and

determining that there is a decryption error when, as a result of the comparing, none of the decryption computation values matches the received comparison computation value.

Claim 16 (Cancelled)